Remarks

Reconsideration of this application is respectfully requested.

Upon entry of the foregoing amendment, claims 1-22 and 26-31 are pending in the application, with claims 1, 6, 10, 16, 26, 29, 30, and 31 being the independent claims. Claims 30 and 31 are sought to be added. No claims are currently amended. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicant respectfully requests that the Examiner reconsider all outstanding rejections and that they be withdrawn.

Claims 1-5

Claims 1-5 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Published Patent Application No. 2002/0172367 to Mulder *et al.* ("Mulder") in view of U.S. Patent No. 6,603,857 to Batten-Carew *et al.* ("Batten-Carew"). Applicant respectfully traverses this rejection.

Claim 1 recites, among other features, *a key store being configured to store a plurality of cryptographic key pairs, each of the cryptographic key pairs includes a public key and a private key, at least one of the cryptographic key pairs pertaining to a predetermined time.*

The Examiner appears to rely on paragraph 0022 of Mulder to allegedly show this feature.

> *In reference to claim 1* Mulder discloses a method fore secure electronic information exchange between a sender and a recipient (abstract). The system of Mulder include a key store (the combination of public key certificate and

> private key storage) that store a plurality of cryptographic key pairs, each of the cryptographic key pairs includes a public key and a private key (paragraph 0022); and an access manager (registration authority) operatively connected to said key store (paragraph 0022), said access manager determines whether the private key of the at least one of the cryptographic key pairs is permitted to be provided to a requester, the user is authenticated (paragraph 0022); (Office Action Page 10; Lines 3-10)

Mulder discloses a method for secure electronic information exchange between a sender and a recipient (Mulder Abstract). In order to receive secure e-documents, the recipient accesses a registration web page via Internet using the recipient's web browser. The recipient is prompted to enter information that is stored in an address book and recipient profile database. Next, a registration authority carries out an authentication of the recipient. After successful authentication, a key generation utility generates a public key and private key pair for the recipient. The private key is archived in the ***private key database*** and the public key is forwarded to a certificate authority to generate a digital public certificate, which includes the recipient's identification information and the public key and is digitally signed. The ***public key certificate*** is stored in the ***public certificate database*** (Mulder Paragraph 0022). Therefore the method of Mulder is directed to using two different databases for storing the keys, the ***private key database*** (Mulder Figure 1, 40) and the ***public certificate database*** (Mulder Figure 1, 36), this is not the same, and is a non-trivial difference compared to, ***a key store*** *being configured to store a plurality of cryptographic key pairs, each of the cryptographic key pairs includes a public key and a private key,* as recited in claim 1.

Moreover, the method of Mulder is directed to archiving the private key and the ***public certificate.*** As discussed above, the public certificate is different than the public key and is generated from the public key and the recipient's information, which is digitally signed (Mulder Paragraph 0022, Lines 22-29 and Figure 2, Step 66). Therefore, the ***public certificate*** that is stored in the ***public certificate database*** is not the same as *a plurality of cryptographic key pairs, each of the cryptographic key pairs includes **a public key** and a private key, at least one of the cryptographic key pairs pertaining to a predetermined time* that is stored in a key store, as recited in claim 1.

Batten-Carew is used to allegedly teach, which Applicants do not acquiesce to, that at least one of the cryptographic key pairs pertains to a predetermined time. Batten-Carew is not used to teach or suggest, nor does Batten-Carew teach or suggest, the aforementioned feature of claim 1. Thus, Batten-Carew fails to cure the deficiencies of Mulder as noted above. Therefore, claim 1 is patentable over Mulder and Batten-Carew taken alone or in combination for at least the reasons provided above because the applied references cannot be used to establish a prima facie case of obviousness.

Furthermore, claims 2-5, all of which depend from independent claim 1, are also patentable over Mulder in view of Batten-Carew for reasons similar to those set forth above with respect to independent claim 1, and further in view of their own respective features.

Claims 10-15

Claims 10-15 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Batten-Carew in view of U.S. Published Patent Application No. 2002/0099947 to Evans ("Evans"), and further in view of U.S. Patent No. 6,951,050 to Singhal *et al.* (“Singhal”). Applicant respectfully traverses this rejection.

Claim 10 recites, among other features, *encrypting the document key using the time-base access key to produce an encrypted document key.*

The Examiner states on page 4 of the Office Action that Batten-Carew does not teach or suggest this recited feature of claim 10. To cure this deficiency, the Examiner relies on Evans (Evans paragraph 0025) to allegedly show this feature.

> Although Batten-Crew discloses obtaining a time-base key, Batten-Carew does not disclose encrypting the data portion of the electronic document using the document key to produce an encrypted data portion; encrypting the document key using the time-base access key to produce an encrypted document key.
>
> Evans discloses encrypting the data portion of the electronic document using the document key to produce an encrypted data portion (paragraph 0025) (Office Action Page 4, Line 18 to Page 5, Line 2)

However, it appears that the Examiner has used Evans to allegedly show the feature *encrypting the data portion of the electronic document using the document key to produce an encrypted data portion* of claim 10, and not the above-noted recited feature of claim 10.

Evans discloses a secure content object that includes an encrypted electronic document, encrypted header, multi-key encryption table and user interface (Evans Para. 0022). The encrypted document is encrypted using a document encryption key. The multi-key encryption table includes at least one multi-key encryption component. A separate component is stored in the table for each authorized user. The combination of user information and the user's multi-key component generates the document key (Evans Para. 0023). Therefore, Evan discloses a method to encrypt an electronic document using a document encrypting key, wherein the document encryption key is generated from a combination of user's multi-key component in the multi-key table and user information. This is not the same as "*encrypting the document key using the time-base access key to produce an encrypted document key,*" as recited in independent claim 10.

Further, Singhal is used to allegedly teach, which Applicant does not acquiesce to, determining whether a time-base access key is already available for a predetermined time, otherwise generating a time based key for the predetermined time. Singhal is not used to teach or suggest, nor does Singhal teach or suggest, the above recited feature of claim 10. Thus, Singhal fails to cure the deficiencies of Batten-Carew as noted above, and Evans, as noted above.

For at least the reasons set forth above, Applicant submits that independent claim 10 is patentable over the combination of Batten-Carew, Evans and Singhal because they cannot be used to establish a prima facie case of obviousness.

Moreover, claims 11-15, all of which depend form independent claim 10, are also patentable over the combination of Batten-Carew, Evans and Singhal for reasons similar to those set forth above with respect to independent claim 10, and further in view of their own respective features.

Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejection of claims 10-15, and find the claims allowable over the applied references.

<u>Claims 16-22</u>

Claims 16-22 were rejected under U.S.C. § 103(a) as allegedly being unpatentable over Evans in view of Batten-Carew. Applicant respectfully traverses this rejection.

Claim 16 recites, among other features, *obtaining an encrypted document key from the header portion of the secured electronic document.*

The Examiner appears to rely on paragraphs 0025 and 0026 of Evans to allegedly show this feature.

> *In reference to claim 16* Mulder discloses a method fore secure electronic information exchange between a sender and recipient (abstract). The system performs a method that includes obtaining an encrypted document key from the header portion of the secured electronic document (paragraph 0025); decrypting an encrypted data portion of the secured electronic document using the document key to produce a data portion (paragraph 0025); and supplying the data portion to the requester (paragraph 0026). (Office Action Page 6, Lines 14-19)

However, upon inspection, nothing in the cited material, or any other portion of Evans, teaches "*obtaining an encrypted document key from the header portion of the secured electronic document,*" as recited in claim 16. Rather, the system of Evans combines user information with multi-key encryption components stored in a multi-key encryption table to generate the document encryption key. The combination of the user information and multi-key component is used to decrypt the encrypted header. If the encrypted header is decrypted successfully, then the correct document key is found (Evans Para. 0025 and Para. 0023). Therefore, as disclosed in Evans, the correct document key is found as a combination of user information and multi-key components, and its validity is checked by decrypting the encrypted header, this is not the same as "*obtaining an encrypted document key from the header portion of the secured electronic document,*" as recited in independent claim 16.

Further, Batten-Carew is used to allegedly teach, which Applicant does not acquiesces to, obtaining a time-base access key and decrypting the encrypted document key using the time-based access key to produce a document key. Batten-Carew is not used to teach or suggest, nor does Batten-Carew teach or suggest, the above recited feature of claim 16. Thus, Batten-Carew fails to cure the deficiencies of Evans as noted above.

Moreover, independent claim 16 is patentable over the applied references for the additional, independent reason that the combination of Evans and Batten-Carew does not teach or suggest *decrypting the encrypted document key using the time-based access key to produce a document key,* as recited in independent claim 16. The Examiner concedes on page 6 of the Office Action that Evans does not teach or suggest the above-noted distinguishing feature of claim 16. To cure this deficiency, the Examiner relies on Batten-Carew (Batten-Carew Fig.3 and column 4 lines 57-65) to allegedly show this feature.

> Evans does not disclose obtaining a time-based access key and decrypting the encrypted document key using the time-based access key to produce a document key.
>
> Batten-Carew discloses a method and apparatus for controlling release of time-sensitive information is accomplished by a server that establishes access information for a specific future time as passed (abstract). The method of Batten-Carew includes obtaining a time-based access key (Fig. 3) and decrypting the encrypted document key using the time-based access key to produce a document key (column 4 line 57-65). (Office Action Page 6, Line 20 to Page 7, Line 5)

However, in the system of Batten-Carew when recipient users obtain a private decryption key, they use the key to decrypt time-sensitive information to obtain the clear text representation thereof (Batten-Carew Col. 3, Line57 to Col. 4, Line 5). This is not the same as using the time-based access key to decrypt the encrypted document key to produce a document key wherein the document key is used to decrypt the data portion of secured electronic document, as recited in claim 16. Therefore, the combination of Evans and Batten-Carew cannot be used to establish a prima facie case of obviousness for claim 16 because the combination of Evans and Batten-Carew fails to disclose each element of claim 16.

For at least the reasons set forth above, Applicant submits that independent claim 16 is patentable over the combination of Evans and Batten-Carew.

Moreover, claims 17-22, all of which depend from independent claim 16, are also patentable over the combination of Evans and Batten-Carew for reasons similar to those set forth above with respect to independent claim 16, and further in view of their own respective features.

Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejection of claims 16-22, and find the claims allowable over the applied references.

Claim 6-9 and 26-29

Claims 6-9 and 26-29 were rejected under U.S.C. § 103(a) as allegedly being unpatentable over Batten-Carew in view of Singhal. Applicant respectfully traverses this rejection.

Claims 6, 26 and 29 recite, among other features, *determining whether a time-based access key is already available for a predetermined time, otherwise generating a time-based access key for the predetermined time*, or similar language.

The Examiner states on page 3 of the Office Action that Batten-Carew does not teach or suggest this recited feature of claims 6, 26, and 29. To cure this deficiency, the

Examiner relies on Singhal (Singhal column 18, lines 30-60) to allegedly show this feature.

> Batten-Carew does not disclose determining whether a time-based access key is already available for a predetermined time, otherwise generating a time-based key for the predetermined time.
>
> Singhal discloses a method, system, and computer program for a secure access techniques to provide user-centric authentication and allow policy-driven packet filtering (abstract). The method a system include determining whether a time-based access key (session key) is already available for a predetermined time, otherwise generating a time-based key for the predetermined time (column 18 lines 30-60). (Office Action Page 3, Lines 6-13)

Singhal discloses methods, systems and computer program instructions for providing location-independent packet routing and secure access in a wireless networking environment, enabling client devices to travel seamlessly within the environment (Singhal Abstract). When a client first communicates with an access point, if no valid ***session key*** already exists between them, a ***session key*** for ***link-level encryption*** is negotiated between them after a successful authentication of the client (Singhal Col. 18, Lines 30-60). The ***session key*** used for ***link-level encryption*** in the system of Singhal is used to ensure that data is not transmitted in clear over the wireless network, but this is not the same as the time-based *access key,* as recited in claims 6, 26, and 29.

For at least the reasons set forth above, Applicant submits that independent claims 6, 26, and 29 are patentable over the combination of Batten-Carew and Singhal.

Furthermore, claims 7-9, all of which depend from independent claim 6, are also patentable over the combination of Batten-Carew and Singhal for reasons similar to those set forth above with respect to independent claim 6, and further in view of their own respective features. In addition, claims 27-28 are also patentable over the combination of Batten-Carew and Singhal for reasons similar to those set forth above with respect to independent claim 26, and further in view of their own respective features.

Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejection of claims 6-9 and 26-29, and find the claims allowable over the applied references.

<u>New Claims 30 and 31</u>

New claims 30 and 31 are computer program claims that recite features similar to claims 10 and 16, and should be found allowable for at least the reasons discussed above.

Conclusion

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Jason D. Eisenberg
Attorney for Applicant
Registration No. 43,447

Date: 1/9/08

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

759903_2.doc